

Physical Layer Security in Cellular Networks: A Stochastic Geometry Approach

He Wang, *Student Member, IEEE*, Xiangyun Zhou, *Member, IEEE*,
Mark C. Reed, *Senior Member, IEEE*

Abstract

This paper studies the information-theoretic secrecy performance in large-scale cellular networks based on a stochastic geometry framework. The locations of both base stations and mobile users are modeled as independent two-dimensional Poisson point processes. We consider two important features of cellular networks, namely, information exchange between base stations and cell association, to characterize their impact on the achievable secrecy rate of an arbitrary downlink transmission with a certain portion of the mobile users acting as potential eavesdroppers. In particular, tractable results are presented under diverse assumptions on the availability of eavesdroppers' location information at the serving base station, which captures the benefit from the exchange of the location information between base stations.

I. INTRODUCTION

During the past decades, we have witnessed the advancement of cellular communication networks. Because of the broadcast nature of the wireless medium, an unauthorized receiver located within the transmission range is capable of eavesdropping the unicast transmissions towards legitimate users, and security is always a crucial issue in cellular systems. Traditionally,

This work was supported by National ICT Australia (NICTA), and the Australian Research Councils Discovery Projects funding scheme (Project No. DP110102548 and DP130101760). NICTA is funded by the Australian Government as represented by the Department of Broadband, Communications and the Digital Economy and the Australian Research Council through the ICT Centre of Excellence program.

H. Wang is with the Research School of Engineering, the Australian National University, ACT 0200, Australia, and also with Canberra Research Laboratory, National ICT Australia, ACT 2601, Australia (e-mail: he.wang@anu.edu.au).

X. Zhou is with the Research School of Engineering, the Australian National University, ACT 0200, Australia (e-mail: xiangyun.zhou@anu.edu.au).

M. C. Reed is with UNSW Canberra, ACT 2600, Australia, and also with the College of Engineering and Computer Science, the Australian National University, ACT 0200, Australia (e-mail: mark.reed@unsw.edu.au).

most of security techniques in modern cellular standards, such as Wideband Code-Division Multiple Access (WCDMA) and Long Term Evolution (LTE), involve means of encryption algorithms in the upper layers of the protocol stacks [1], [2]. In contrast, the concept of achieving information-theoretic security by protecting the physical layer of wireless networks has attracted attention widely in the research community. Wyner proposed the wiretap channel model and the notion of perfect secrecy for point-to-point communication in his pioneering work [3], which was extended to broadcast channels with confidential messages by Csiszár and Körner [4]. Based on these initial results, a positive secrecy capacity, defined as the maximum transmission rate at which the eavesdropper is unable to obtain any information, can be achieved if the intended receiver enjoys a better channel than the potential eavesdropper.

Unlike point-to-point scenarios, the communication between nodes in large-scale networks strongly depends on the location distribution and the interactions between nodes. Based on the assumption that legitimate nodes and eavesdroppers are distributed randomly in the space, the studies on the secure communications for large-scale wireless networks have been carried out recently, from the information-theoretic viewpoint. Secrecy communication graphs describing secure connectivity over a large-scale network with eavesdroppers present were investigated in [5]–[8]. In particular, the statistical characterizations of in-degree and out-degree under the security constraints were considered by Haenggi [5], Pinto *et al.* [6] and Goel *et al.* [7]. By using the tools from percolation theory, the existence of a secrecy graph was analyzed in [5], [8]. The results in [9] showed the improvements in the secure connectivity by introducing directional antenna elements and eigen-beamforming. In order to derive the network throughput, these works on connectivity were further extended for secrecy capacity analysis. Specifically, the maximum achievable secrecy rate under the worst-case scenario with colluding eavesdroppers was given in [10]. Scaling laws for secrecy capacity in large networks have been investigated in [11]–[13]. Focusing on the transmission capacity of secure communications, the throughput cost of achieving a certain level of security in an interference-limited network was analyzed in [14], [15]. It should be noticed that all works mentioned above were concentrated on ad hoc networks.

A. Approach and Contributions

In this work, we focus on the secrecy performance in large-scale cellular networks, considering cellular networks' unique characteristics different from ad hoc networks: the carrier-operated high-speed backhaul networks connecting individual base stations (BSs) and the

core-network infrastructures, which provide us potential means of BS cooperation, such as associating mobile users to the optimal BS with secrecy considerations and exchanging information to guarantee better secure links.

Fortunately, modeling BSs to be randomly placed points in a plane and utilizing stochastic geometry [16], [17] to analyze cellular networks have been used extensively as an analytical tool for improving tractability [18]–[20]. Recent works [21]–[25] have shown that the network models with BS locations drawn from a homogeneous Poisson point process (PPP) are as accurate as the traditional grid models compared with the result of an practical network deployment, and can provide more tractable analytical results which give pessimistic lower bounds on coverage and throughput. For these reasons we adopt PPPs to model the locations of BSs of the cellular networks in this paper.

The following scenario of secure communication in cellular networks is considered in this work: confidential messages are prepared to be conveyed to a mobile user, while certain other mobile users should not have the access to the messages and hence are treated as potential eavesdroppers. The serving BS should ensure the messages delivered to the intended user successfully while keeping perfect secrecy against all potential eavesdroppers. Considering the fact that the cellular service area is divided into cells, each BS knows the location as well as the identity of each user (i.e., whether the user is a potential eavesdropper or not) in its own cell. The identity and location information of mobile users in the other cells can be obtained by information exchange between BSs via the backhaul networks.

The main contributions of this paper are as follows:

- First, our analytical results quantify the secrecy rate performance in large-scale cellular networks. Specifically, tractable results are provided on the probability distribution of the secrecy rate and hence the average secrecy rate achievable for a randomly located mobile user in such a cellular network, under different assumptions on the cell association and location information exchange between BSs as follows:
 - *Scenario-I*: the serving BS fully acquires potential eavesdroppers' location information; the nearest BS from the intended user is chosen as the serving BS.
 - *Scenario-II*: the serving BS fully acquires potential eavesdroppers' location information; the BS providing best secrecy performance at the intended user is chosen as the serving BS.
 - *Scenario-III*: the serving BS partially acquires potential eavesdroppers' location information; the nearest BS from the intended user is associated as the serving BS.

- In addition, a unique feature of secure transmissions that the optimal BS is often not the nearest BS is identified and analyzed in the work. Our results show that only marginal gain can be obtained by optimally choosing the serving BS rather than associating to the nearest one. In other words, keeping the nearest BS to be used for secure transmission still achieves near-optimal secrecy performance, which is a very useful message to the network designers.
- Finally, our analysis sheds light into the impact of the availability of eavesdroppers' location information on the achievable secrecy rate. In particular, the secrecy performances for the scenarios with no location information exchange and limited exchange with neighboring cells are derived, which demonstrate the critical role of this kind of BS cooperation. This result provides network designers with practical guidelines in deciding on the necessary information exchange range, i.e., how many nearby BSs should participate in the information exchange for achieving a certain level of secrecy performance.

It should be noted that similar work to evaluate secrecy performance of large-scale cellular networks was conducted in [26]; however, it mainly focused on the scaling behavior of the eavesdropper's density to allow full coverage over the entire network, without taking the achievable secrecy rate into account. In contrast, we characterize the statistics of the secrecy rate at an arbitrary mobile user under different cell association models and eavesdroppers' location information exchanging assumptions mentioned above.

The remainder of the paper is organized as follows: In Section II, we present the system model and general assumptions in this work. Section III shows the main result of this paper, in which we obtain simple tractable expressions for achievable secrecy rates under different scenarios. Section IV provides numerical results and concluding remarks are given in Section V.

II. SYSTEM MODEL

We consider the downlink scenario of a cellular network utilizing an orthogonal multiple access technique and composed of a single class of BSs, macro BS for instance. We focus on the performance achieved by a randomly chosen typical mobile user. The BSs are assumed to be spatially distributed as a two-dimensional homogeneous PPP Φ_{BS} of density λ_{BS} , and all BSs have the same transmit power value P_{BS} . An independent collection of mobile users, located according to an independent homogeneous PPP Φ_{MS} of density λ_{MS} , is assumed.

We consider the process $\Phi_{MS} \cup \{0\}$ obtained by adding a user at the origin of the coordinate system. By Slivnyak's Theorem [16], this user can be taken as the typical user, since adding a user is identical to conditioning on a user at that location.

A. Signal Model

The standard power loss propagation model is used with path loss exponent $\alpha > 2$. Hence, the received power at the receiver x_i from the transmitter x_j is written as

$$P_{rx}(x_i, x_j) = P_{BS} \|x_i - x_j\|^{-\alpha}. \quad (1)$$

The noise power is assumed to be additive and constant with value σ^2 for all users, but no specific distribution is assumed.

In this work, we assume that there is no in-band interference at downlink receivers. This assumption is achievable by a carefully planned frequency reuse pattern, where the interfering BSs are far away to have the serving BS occupying some resource blocks exclusively in a relatively large region, and the interference can be incorporated in the constant noise power.

B. Achievable Secrecy Rate

We consider a scenario where confidential messages are prepared to be delivered to the typical user, while certain individuals among other mobile users, treated as potential malicious eavesdroppers (or called Eve for brevity) by the network, should be kept from accessing them. We model a fraction of the other mobile users randomly chosen from Φ_{MS} (the process constructed by all other users except the typical user) as the eavesdroppers, i.e., a thinned PPP with the density of λ_e , denoted by Φ_e .

Here we assume that each BS knows both the location and the identity (i.e., whether the user is a potential eavesdropper or not) of each mobile user in its own cell, and the cell of each BS is the Voronoi cell containing the BS, where the Voronoi tessellation is formed by PPP Φ_{BS} [16], as shown in Fig. 1. The identity and location information of mobile users in the other Voronoi cells can be obtained by the information exchange between BSs via backhaul networks.

Firstly, if we suppose the ideal case where the serving BS located at x knows the locations of all eavesdroppers in the plane, which requires that the location and identity information of all users is shared completely through the backhaul network, the maximum secrecy rate

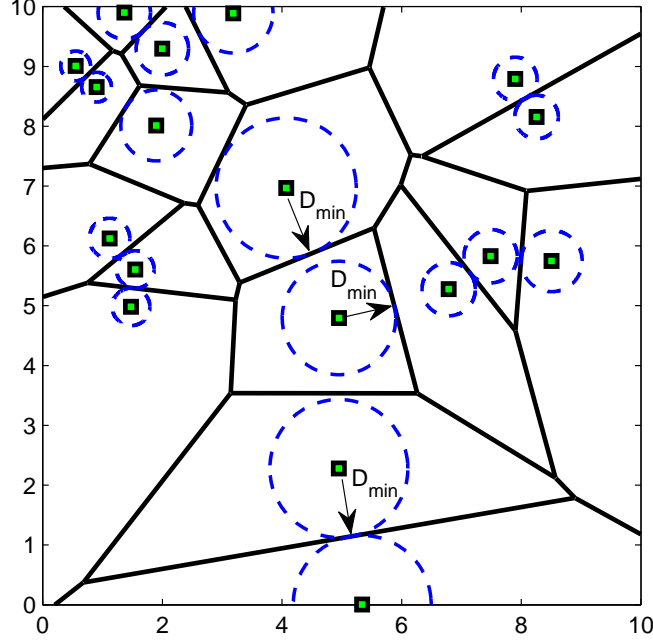


Fig. 1. Illustration of Poisson distributed BSs' cell boundaries. Each user is associated with the nearest BS, and BSs (represented by green squares) are distributed according to PPP. D_{\min} is defined as BS's minimum distance to its cell boundaries.

achievable at the typical mobile user is given by [6], [27], as

$$R_s = \max \left\{ \log_2 \left(1 + \frac{P_{rx}(0, x)}{\sigma^2} \right) - \log_2 \left(1 + \frac{P_{rx}(e^*(x), x)}{\sigma^2} \right), 0 \right\}, \quad (2)$$

where

$$e^*(x) = \arg \max_{e \in \Phi_e} P_{rx}(e, x) = \arg \min_{e \in \Phi_e} \|e - x\|, \quad (3)$$

i.e., $e^*(x)$ is the location of the most detrimental eavesdropper, which is the nearest one from the serving BS in this case.

Then, assuming limited information exchange between BSs, there will be regions in which the eavesdroppers' location information is unknown to the serving BS, which is denoted by $\Theta \subset \mathbb{R}^2$. When this happens, the serving BS assumes the worst case, i.e., eavesdroppers can lie at any points in Θ . Then the achievable secrecy rate is still given by (2), but $e^*(x)$ should be

$$e^*(x) = \arg \max_{e \in \Phi_e \cup \Theta} P_{rx}(e, x), \quad (4)$$

where the detrimental eavesdropper is chosen from the union of the eavesdropper set Φ_e and the unknown region Θ .

It should be noticed that the randomness introduced by Φ_{BS} and Φ_e makes the achievable secrecy rate R_s at the typical user a random variable. Furthermore, the distribution of R_s is mixed, i.e., R_s has a continuous distribution on $(0, \infty)$ and a discrete component at 0. For $R_s \in (0, \infty)$, the complementary cumulative distribution function (CCDF) of R_s is given as

$$\bar{F}_{R_s}(R_0) = \mathbb{P}\left(\log_2\left(1 + \frac{P_{rx}(0, x)}{\sigma^2}\right) - \log_2\left(1 + \frac{P_{rx}(e^*(x), x)}{\sigma^2}\right) > R_0\right), \text{ for } R_0 \geq 0. \quad (5)$$

For the special case of $R_s = 0$, it has the probability $\mathbb{P}(R_s = 0) = 1 - \bar{F}_{R_s}(0)$, which corresponds to the probability that the link to the typical user cannot support any positive secrecy rate.

By assuming that the receivers of both the legitimate user and eavesdroppers operate in the high signal-to-noise ratio (SNR) regime, i.e., $P_{rx}(0, x)/\sigma^2 \gg 1$ and $P_{rx}(e^*(x), x)/\sigma^2 \gg 1$, we can obtain an approximation of R_s , denoted by \hat{R}_s , i.e., $\hat{R}_s = \max\{\log_2(P_{rx}(0, x)/\sigma^2) - \log_2(P_{rx}(e^*(x), x)/\sigma^2), 0\}$, the CCDF of which is

$$\begin{aligned} \bar{F}_{\hat{R}_s}(R_0) &= \mathbb{P}\left(\frac{P_{rx}(0, x)}{P_{rx}(e^*(x), x)} > \beta\right) \\ &= \mathbb{P}\left(\|e^*(x) - x\| > \beta^{1/\alpha}\|x\|\right), \text{ for } R_0 \geq 0, \end{aligned} \quad (6)$$

where the threshold β is defined as $\beta \triangleq 2^{R_0}$. In this work, we focus on high SNR scenarios and use the above expression to obtain tractable results on the secrecy rate performance. The obtained analytical results give approximations on the secrecy performance at finite SNR values.

Furthermore, from the fact that the achievable secrecy rate R_s should always be non-negative, we can easily reach the conclusion that the high SNR approximation $\bar{F}_{\hat{R}_s}(R_0)$ serves as an upper bound for the CCDF of R_s at finite SNR, i.e.,

$$\begin{aligned} \bar{F}_{R_s}(R_0) &= \mathbb{P}\left(\frac{\sigma^2 + P_{rx}(0, x)}{\sigma^2 + P_{rx}(e^*(x), x)} > 2^{R_0}\right) \\ &\leq \mathbb{P}\left(\frac{P_{rx}(0, x)}{P_{rx}(e^*(x), x)} > 2^{R_0}\right) = \bar{F}_{\hat{R}_s}(R_0), \text{ for } R_0 \geq 0, \end{aligned} \quad (7)$$

where the two probability expressions are equal when $R_0 = 0$. Therefore, some of our analytical results on $\bar{F}_{\hat{R}_s}(R_0)$ and $\mathbb{E}[\hat{R}_s]$ under the high SNR assumption, including the exact expressions and upper bounds, give valid upper bounds on the secrecy performances at finite SNR values.

III. MAIN RESULTS

In this section, we provide the main results on the probabilistic characteristics of the achievable secrecy rates \hat{R}_s and the average secrecy rates achievable $\mathbb{E}[\hat{R}_s]$ under three major scenarios, where different criteria to choose the serving BS are used and the serving BS can fully or partially acquire the location information of the eavesdroppers, corresponding to the different levels of BS cooperation introduced. It should be noticed that the BS cooperation considered in this paper includes only exchanging the identity and location information of the mobile users and selecting the appropriate BS to serve the typical user.

A. Scenario-I: Full Location Information; Nearest BS to Serve

We firstly assume that the location information of all eavesdroppers can be fully accessed by the serving BS and employ the cell association model by confining mobile users to be served by the nearest BS only. The location and identity information of mobile users in the serving BS's cell can be obtained easily, and other users' information is supplied by other BSs via the backhaul networks. Associating users to the nearest BS is commonly used in related cellular modeling works [18], [21], and equivalently it means that a BS is associated with the users in its Voronoi cell (formed by the PPP Φ_{BS}).

Proposition 1. *Under the conditions of mobile users being served by the nearest BS and the availability of full location information for all eavesdroppers, the CCDF of the achievable secrecy rate obtained at the typical user is given by*

$$\bar{F}_{\hat{R}_s}(R_0) = \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2R_0)/\alpha}}, \text{ for } R_0 \geq 0. \quad (8)$$

Proof: Here we use x_0 to denote the nearest BS from the origin, and we define r_u as the distance from the typical user to the nearest BS, namely, $r_u = \|x_0\|$. The probability density function (pdf) of r_u has been provided in [28], as

$$f_{r_u}(r) = 2\pi\lambda_{BS}r \exp(-\pi\lambda_{BS}r^2). \quad (9)$$

Due to the assumption that the serving BS knows all eavesdroppers' locations in this scenario, the most detrimental eavesdropper $e^*(x_0)$ for the BS at x_0 should be the nearest one from x_0 , as given in (3). We define the (closed) ball centered at p and of radius r as $\mathcal{B}(p, r)$, i.e., $\mathcal{B}(p, r) \triangleq \{m \in \mathbb{R}^2, \|m - p\| \leq r\}$. Then the CCDF of the achievable secrecy rate \hat{R}_s under this scenario can be derived as

$$\bar{F}_{\hat{R}_s}(R_0) = \mathbb{P}\left(\|e^*(x_0) - x_0\| > \beta^{1/\alpha}\|x_0\|\right)$$

$$\begin{aligned}
&= \int_0^\infty \mathbb{P}(\|e^*(x_0) - x_0\| > \beta^{1/\alpha} r_u \mid r_u = y) f_{r_u}(y) dy \\
&= \int_0^\infty \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{1/\alpha} r_u) \mid r_u = y] f_{r_u}(y) dy \\
&\stackrel{(a)}{=} \int_0^\infty \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{1/\alpha} y)] f_{r_u}(y) dy \\
&\stackrel{(b)}{=} \int_0^\infty \exp(-\pi \lambda_e \beta^{2/\alpha} y^2) \cdot 2\pi \lambda_{BS} y \exp(-\pi \lambda_{BS} y^2) dy \\
&= \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2R_0)/\alpha}}, \tag{10}
\end{aligned}$$

where step (a) is derived based on the independence between Φ_e and Φ_{BS} , and step (b) follows the PPP's void probability and pdf of r_u given in (9). Through the deduction above, the CCDF expression of the achievable secrecy rate can be obtained. ■

Corollary 1. *Under the conditions of mobile users being served by the nearest BS and the availability of full location information for all eavesdroppers, the average secrecy rate achievable at the typical user is provided by*

$$\mathbb{E}[\hat{R}_s] = \frac{\alpha}{2 \ln 2} \cdot \ln \left(\frac{\lambda_{BS} + \lambda_e}{\lambda_e} \right). \tag{11}$$

Proof: Based on the CCDF expression given in Proposition 1, the average secrecy rate achievable at the typical user can be obtained by integrating (8) from 0 to ∞ , i.e.,

$$\begin{aligned}
\mathbb{E}[\hat{R}_s] &= \int_0^\infty \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2t)/\alpha}} dt \\
&\stackrel{(a)}{=} \left[\frac{1}{\ln(2^{2/\alpha})} \cdot \ln \left(\frac{\exp[\ln(2^{2/\alpha})t]}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot \exp[\ln(2^{2/\alpha})t]} \right) \right]_0^\infty \\
&= \frac{\alpha}{2 \ln 2} \ln \left(\frac{1}{\lambda_e/\lambda_{BS}} \right) - \frac{\alpha}{2 \ln 2} \ln \left(\frac{1}{1 + \lambda_e/\lambda_{BS}} \right) \\
&= \frac{\alpha}{2 \ln 2} \cdot \ln \left(\frac{\lambda_{BS} + \lambda_e}{\lambda_e} \right), \tag{12}
\end{aligned}$$

where step (a) follows the indefinite integral result for the form of the integrand herein, which can be found in [29]. ■

B. Scenario-II: Full Location Information; Optimal BS to Serve

Next, we still keep the assumption that the serving BS has all eavesdroppers' location information, which can be achieved by an ideal information exchange between BSs; however, in this scenario, we assume that all BSs can act as candidates to serve the typical user.

This scenario provides us the maximum achievable secrecy rate from the information-theoretic point of view, which tells the network designer the ultimate secrecy performance the cellular network can offer and can be viewed as the optimal BS cooperation scheme considered in this paper. Obviously, to obtain the optimal secrecy performance, the BS achieving the maximum secrecy rate should be selected. By studying the secrecy performance with the optimal cell association, we are able to quantify the gap between the secrecy performances provided by the optimal BS and the nearest BS.

Based upon these assumptions, the achievable secrecy rate at the typical user becomes

$$\hat{R}_s = \max \left\{ \max_{x \in \Phi_{BS}} \left\{ \log_2 \left(\frac{P_{rx}(0, x)}{\sigma^2} \right) - \log_2 \left(\frac{P_{rx}(e^*(x), x)}{\sigma^2} \right) \right\}, 0 \right\}, \quad (13)$$

where $e^*(x)$ is given by (3).

Proposition 2. *Under the conditions of mobile users being served by the optimal BS and the availability of full location information for all eavesdroppers, an upper bound for the CCDF of the achievable secrecy rate at the typical user is given by*

$$\bar{F}_{\hat{R}_s}(R_0) \leq 1 - \exp \left(- \frac{\lambda_{BS}}{\lambda_e 2^{(2R_0)/\alpha}} \right), \text{ for } R_0 \geq 0, \quad (14)$$

and a lower bound is given by

$$\bar{F}_{\hat{R}_s}(R_0) \geq \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2R_0)/\alpha}}, \text{ for } R_0 \geq 0. \quad (15)$$

Proof: For a given BS (not necessarily the nearest BS) located at the position of x , its achievable secrecy rate toward the origin's typical user is larger than R_0 if and only if there is no eavesdroppers located within $\mathcal{B}(x, 2^{(R_0/\alpha)} \|x\|)$. Hence, the achievable secrecy rate's cumulative distribution function (CDF) can be derived as

$$\begin{aligned} F_{\hat{R}_s}(R_0) &= \mathbb{P}(\hat{R}_s \leq R_0) \\ &= \mathbb{P}[\text{All BSs can not provide secrecy rate larger than } R_0] \\ &= \mathbb{E}_{\Phi_e} \left[\mathbb{E}_{\Phi_{BS}} \left[\prod_{x \in \Phi_{BS}} \mathbf{1}\{\Phi_e \cap \mathcal{B}(x, 2^{\frac{R_0}{\alpha}} \|x\|) \neq \emptyset\} \right] \right] \\ &= \mathbb{E}_{\Phi_e} \left[\mathbb{E}_{\Phi_{BS}} \left[\prod_{x \in \Phi_{BS}} \left[1 - \mathbf{1}\{\Phi_e \cap \mathcal{B}(x, 2^{\frac{R_0}{\alpha}} \|x\|) = \emptyset\} \right] \right] \right] \\ &\stackrel{(a)}{=} \mathbb{E}_{\Phi_e} \left[\exp \left[- \lambda_{BS} \int_{\mathbb{R}^2} \mathbf{1}\{\Phi_e \cap \mathcal{B}(x, 2^{\frac{R_0}{\alpha}} \|x\|) = \emptyset\} dx \right] \right] \\ &\geq \exp \left[- \lambda_{BS} \int_{\mathbb{R}^2} \mathbb{P}[\Phi_e(\mathcal{B}(x, 2^{\frac{R_0}{\alpha}} \|x\|)) = \emptyset] dx \right], \end{aligned} \quad (16)$$

where $R_0 \geq 0$, step (a) follows from the probability generating functional (PGFL) of the PPP [16], and Jensen's inequality gives the lower bound for $F_{\hat{R}_s}(R_0)$ in the last step. The part in the integral can be derived by using 2-D homogeneous PPP's void probability [16], i.e., $\mathbb{P}[\Phi_e(\mathcal{B}(x, 2^{(R_0/\alpha)}\|x\|)) = 0] = \exp(-\pi\lambda_e 2^{(2R_0/\alpha)}\|x\|^2)$, which can be substituted into the integration in (16) to obtain the upper bound of the achievable secrecy rate's CCDF in (14) easily.

Then we turn to find the lower bound for the CCDF of the achievable secrecy rate. Here we use $\hat{R}_{s,nearest}$ to denote the achievable secrecy rate where only the nearest BS is accessible, which has been studied in Scenario-I. Since connecting to the nearest BS is always one of the viable options if all BSs are reachable, we can have the usual stochastic order between $\hat{R}_{s,nearest}$ in Scenario-I and \hat{R}_s in the current scenario, i.e., $\mathbb{P}(\hat{R}_{s,nearest} > R_0) \leq \mathbb{P}(\hat{R}_s > R_0)$ or equivalently $\bar{F}_{\hat{R}_s}(R_0) \geq \bar{F}_{\hat{R}_{s,nearest}}(R_0)$. Therefore, the conclusion in Proposition 1 provides the lower bound in (15), which completes the proof. ■

Proposition 3. *Under the conditions of mobile users being served by the optimal BS and the availability of full location information for all eavesdroppers, another upper bound for the CCDF of the achievable secrecy rate at the typical user is given by*

$$\bar{F}_{\hat{R}_s}(R_0) \leq 1 - \mathbb{E}_{V_d} \left[\exp \left(- \frac{4}{(1 + 2^{R_0/\alpha})^2} \cdot \frac{\lambda_{BS}}{\lambda_e} \cdot V_d \right) \right], \text{ for } R_0 \geq 0, \quad (17)$$

where the expectation is taken over the random variable V_d , the area of the typical Voronoi cell of a PPP with the unitary density.

Proof: For the set of eavesdropper locations Φ_e , we can define a random set \mathcal{P} , the union of all points at which BS can provide the typical user (at the origin) a secrecy rate $\hat{R}_s > R_0$, i.e.,

$$\mathcal{P} = \left\{ x \in \mathbb{R}^2 : \|e - x\| > \beta^{1/\alpha} \|x\|, \forall e \in \Phi_e \right\}, \quad (18)$$

which is based upon the assumption that the serving BS knows all eavesdroppers' locations in this scenario. Furthermore, we define \mathcal{C} as the Voronoi cell generated by the process $\Phi_e \cup \{0\}$, the union of the eavesdroppers' locations and the origin. Because of Slivnyak's Theorem, the Voronoi cell around the origin formed by $\Phi_e \cup \{0\}$ has the same property as a randomly chosen Voronoi cell formed by a PPP with density λ_e . The area measures of the random set \mathcal{P} and \mathcal{C} are denoted by $A(\mathcal{P})$ and $A(\mathcal{C})$ respectively. An example of these random sets is illustrated in Fig. 2, in which we can obtain a straightforward relationship between $A(\mathcal{P})$

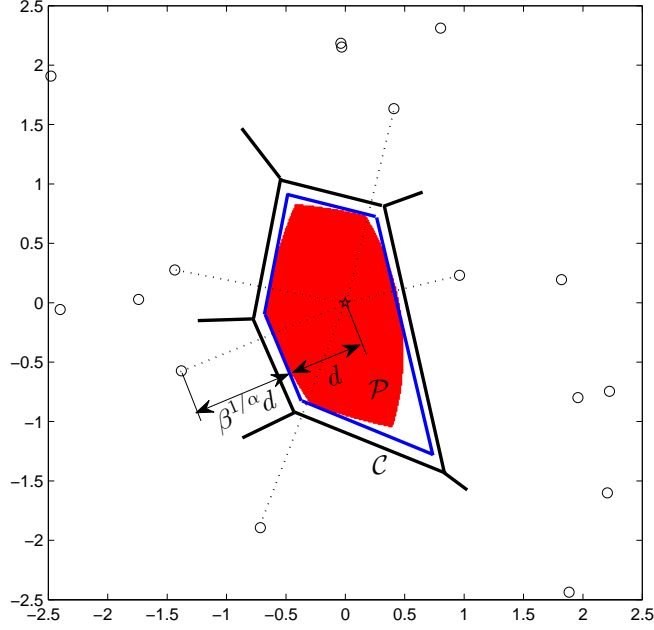


Fig. 2. Illustration of the relationship between \mathcal{P} (the union of all points at which BS can provide the typical user a secrecy rate $\hat{R}_s > \log_2(\beta)$, where $\beta = 1.25$, represented as the red region) and \mathcal{C} (the Voronoi cell generated by the process $\Phi_e \cup \{0\}$), as defined in the proof of Proposition 3. The typical user denoted by a star is located at the origin. A realization of eavesdroppers are scattered and denoted as circles.

and $A(\mathcal{C})$ as

$$A(\mathcal{P}) \leq \frac{4}{(1 + \beta^{1/\alpha})^2} A(\mathcal{C}), \quad (19)$$

if $\beta \geq 1$ or equivalently $R_0 \geq 0$.

The value $[4/(1 + \beta^{1/\alpha})^2] A(\mathcal{C})$ is the area measure of the region enclosed by blue lines in Fig. 2, which is the exact shape shrunk from \mathcal{C} and has edges tangential to \mathcal{P} 's edges. Obviously, for a realization of the BS location Φ_{BS} , the typical user can have a secrecy rate larger than R_0 if and only if there is at least a BS located in \mathcal{P} , which makes the CCDF of the secrecy rate \hat{R}_s become

$$\begin{aligned} \bar{F}_{\hat{R}_s}(R_0) &= \mathbb{P}[\text{No BS exists in } \mathcal{P}] \\ &\stackrel{(a)}{=} 1 - \mathbb{E}_{\mathcal{P}} \left[\exp(-\lambda_{BS} A(\mathcal{P})) \right] \\ &\leq 1 - \mathbb{E}_{\mathcal{P}} \left[\exp\left(-\frac{4\lambda_{BS}}{(1 + \beta^{1/\alpha})^2} A(\mathcal{C})\right) \right] \\ &= 1 - \mathbb{E}_{V_d} \left[\exp\left(-\frac{4}{(1 + \beta^{1/\alpha})^2} \cdot \frac{\lambda_{BS}}{\lambda_e} \cdot V_d\right) \right], \end{aligned} \quad (20)$$

where the expectation in step (a) is taken over the random set \mathcal{P} . ■

Remark: It can be observed that the upper bound obtained in Proposition 3 depends on the statistic characteristics of Voronoi cell's area. It provides us an accurate approximation for small positive \hat{R}_s values and complements the upper bound result in Proposition 2. Particularly, for the special case of $R_0 = 0$, the region \mathcal{P} turns out to be the Voronoi cell \mathcal{C} , thus making the CCDF upper bound become the exact result, i.e.,

$$\bar{F}_{\hat{R}_s}(0) = 1 - \mathbb{E}_{V_d} \left[\exp \left(- \frac{\lambda_{BS}}{\lambda_e} V_d \right) \right], \quad (21)$$

and the expression in this extreme case is consistent with the secrecy coverage probability provided in [26]. For high value of R_0 , however, the area difference between $A(\mathcal{P})$ and $[4/(1 + \beta^{1/\alpha})^2] A(\mathcal{C})$ increases, which makes the approximation in (19) become imprecise. This can explain the numerical results we will observe later in Fig. 5, i.e., the discrepancy between the upper bound given by Proposition 3 and the simulation result for $R_0 = 5$.

Although there is no known closed form expression of V_d 's pdf [30], some accurate estimates of this distribution were produced in [31], [32]. For instance, a simple gamma distribution was used to fit the pdf of V_d derived from Monte Carlo simulations in [32], i.e.,

$$f_{V_d}(x) \approx b^q x^{q-1} \exp(-bx) / \Gamma(q), \quad (22)$$

where $q = 3.61$, $b = 3.61$ and $\Gamma(x) = \int_0^\infty t^{x-1} e^{-t} dt$ is the standard gamma function. By substituting this estimate into (17) and simplifying the integral, we can obtain

$$\bar{F}_{\hat{R}_s}(R_0) \approx 1 - \frac{b^q}{\left(b + \frac{4}{(1+2R_0/\alpha)^2} \cdot \frac{\lambda_{BS}}{\lambda_e}\right)^q}, \text{ for } R_0 \geq 0. \quad (23)$$

After giving the bounds for \hat{R}_s 's CCDF, we will focus on the average secrecy rate achievable for a randomly located user.

Corollary 2. *Under the conditions of mobile users being served by the optimal BS and the availability of full location information for all eavesdroppers, an upper bound of the average secrecy rate achievable at the typical user is provided by*

$$\mathbb{E}[\hat{R}_s] \leq \frac{\alpha}{2 \ln 2} \cdot \left[\gamma + \ln \left(\frac{\lambda_{BS}}{\lambda_e} \right) + E_1 \left(\frac{\lambda_{BS}}{\lambda_e} \right) \right], \quad (24)$$

and a lower bound is provided by

$$\mathbb{E}[\hat{R}_s] \geq \frac{\alpha}{2 \ln 2} \cdot \ln \left(\frac{\lambda_{BS} + \lambda_e}{\lambda_e} \right), \quad (25)$$

where $E_1(x) = \int_x^\infty \exp(-t) \frac{1}{t} dt$ is the exponential integral and γ is the Euler-Mascheroni constant.

Proof: Based on the CCDF bounds given in Proposition 2, the upper and lower bound of the average secrecy rate achievable at the typical user can be obtained by integrating (14) and (15) from 0 to ∞ . Specifically, the upper bound can be derived as

$$\begin{aligned}\mathbb{E}[\hat{R}_s] &\leq \int_0^\infty \left[1 - \exp\left(-\frac{\lambda_{BS}}{\lambda_e 2^{(2t)/\alpha}}\right)\right] dt \\ &\stackrel{(a)}{=} \frac{1}{\ln(2^{2/\alpha})} \int_0^{\frac{\lambda_{BS}}{\lambda_e}} \frac{1 - \exp(-v)}{v} dv,\end{aligned}\quad (26)$$

where step (a) is derived by employing a change of variables $v = \lambda_{BS}/(\lambda_e 2^{(2t)/\alpha})$. We use the Taylor series expansion of $\exp(-v)$, and the integrand in (26) becomes

$$\frac{1 - \exp(-v)}{v} = \sum_{k=1}^{\infty} \frac{(-v)^{k-1}}{k!}.\quad (27)$$

Then by integrating both sides of the equation (27) and performing simple mathematical operations, we can obtain the relationship

$$\begin{aligned}\int_0^{\frac{\lambda_{BS}}{\lambda_e}} \frac{1 - \exp(-v)}{v} dv &= \int_0^{\frac{\lambda_{BS}}{\lambda_e}} \sum_{k=1}^{\infty} \frac{(-v)^{k-1}}{k!} dv \\ &= \sum_{k=1}^{\infty} \int_0^{\frac{\lambda_{BS}}{\lambda_e}} \frac{(-v)^{k-1}}{k!} dv \\ &= -\sum_{k=1}^{\infty} \frac{(-\frac{\lambda_{BS}}{\lambda_e})^k}{k \cdot k!}.\end{aligned}\quad (28)$$

Since the exponential integral can be expressed as $E_1(x) = -\gamma - \ln(x) + \sum_{k=1}^{\infty} \frac{(-1)^{k+1} x^k}{k \cdot k!}$ when $x > 0$ [33], the above integral can be derived as

$$\int_0^{\frac{\lambda_{BS}}{\lambda_e}} \frac{1 - \exp(-v)}{v} dv = \gamma + \ln\left(\frac{\lambda_{BS}}{\lambda_e}\right) + E_1\left(\frac{\lambda_{BS}}{\lambda_e}\right).\quad (29)$$

Plugging (29) into (26) gives the upper bound of the average secrecy rate in (24).

On the other hand, following the same procedure as the one to prove Corollary 1, the lower bound of average secrecy rate can be obtained, which completes the proof. ■

An alternative upper bound of the average secrecy rate achievable can be derived based upon Proposition 3, and the corresponding performance will also be shown in Section IV.

It should be noticed that the optimal BS mentioned here is not necessarily the nearest BS, since it is possible that other BSs can provide higher secrecy rate than the nearest BS. Taking the case illustrated in Fig. 3 for example, the typical user's nearest BS is BS-A, which, however, is hardly capable of providing a secure connection due to its excellent connection to the eavesdropper nearby. Alternatively, choosing BS-B to serve can provide a certain level

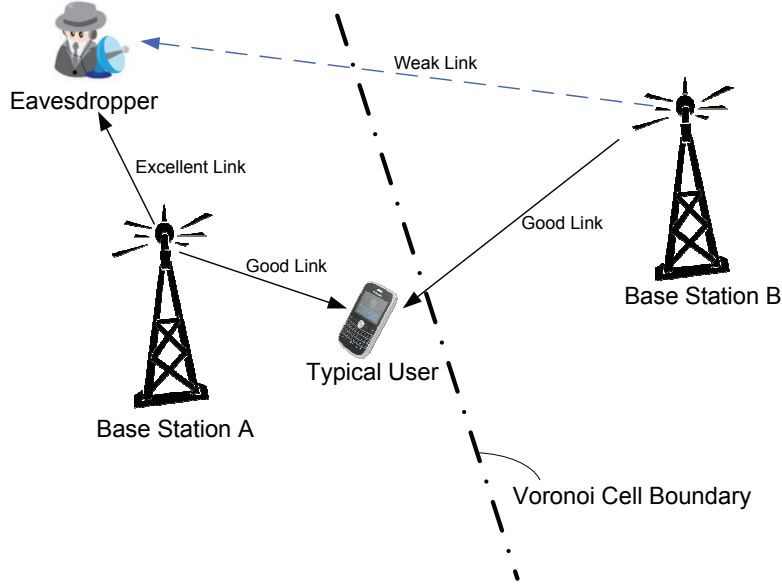


Fig. 3. An example where the BS providing maximum achievable secrecy rate is not the nearest BS. The typical user's nearest BS is BS-A, which however cannot provide a positive secrecy rate due to its excellent link to the eavesdropper. BS-B, on the other hand, can provide a secrecy connection since there is no eavesdroppers nearby.

secrecy rate if the typical user's channel quality to BS-B is better than the channel to the eavesdropper.

By comparing the secrecy performance in Scenario-I (the typical user served by the nearest BS) with this scenario (the typical user served by the best BS), we will be able to see the benefit from optimally choosing the serving BS to provide the secure downlink transmission. The numerical illustrations will be provided in Section IV.

C. Scenario-III: Limited Location Information; Nearest BS to Serve

Here we still assume the same cell association model as Scenario-I, i.e., mobile users are served by the nearest BS, nevertheless only limited users' location and identity information is known to the serving BS. Considering the backhaul bandwidth cost in practice and the core-network implementation complexity for BS cooperation, the scenarios where the location and identity information is only exchanged with neighboring cells or even no exchange allowed at all are analyzed in this section.

1) *No location and identity information exchange:* Firstly, we assume that no location and identity information exchange allowed between BSs, which means that the serving BS only knows the intracell users' location and identity information. As mentioned in section II-B, the

unknown region outside the serving cell leads to the worst case assumption that eavesdroppers lie on the serving BS's cell boundaries and limit the achievable secrecy rate.

Before coming to this scenario's secrecy performance, we firstly define the minimum distance from PPP's each point to its own cell boundaries, denoted as D_{\min} . In Fig. 1, for instant, the D_{\min} of three BSs are illustrated. In the cell tessellation formed by BS PPP with density λ_{BS} , we can simply use the void probability of a PPP to derive

$$\begin{aligned}\mathbb{P}(D_{\min} > r) &= \mathbb{P}[\text{No BS closer than } 2r] \\ &= e^{-\pi\lambda_{BS}(2r)^2}.\end{aligned}\quad (30)$$

Therefore, the CDF is $F_{D_{\min}}(r) = \mathbb{P}(D_{\min} \leq r) = 1 - e^{-\pi\lambda_{BS}(2r)^2}$ and the pdf can be found as

$$f_{D_{\min}}(r) = \frac{dF_{D_{\min}}(r)}{dr} = 8\pi\lambda_{BS}r \exp(-4\pi\lambda_{BS}r^2). \quad (31)$$

Proposition 4. *Under the conditions of mobile users being served by the nearest BS and only intracell eavesdroppers' location information available, a lower bound for the CCDF of the achievable secrecy rate obtained at the typical user is given by*

$$\bar{F}_{\hat{R}_s}(R_0) \geq \frac{1}{1 + (\frac{\lambda_e}{\lambda_{BS}} + 4) \cdot 2^{(2R_0)/\alpha}}, \text{ for } R_0 \geq 0. \quad (32)$$

Proof: Based on the available intracell eavesdroppers' location information and the assumption that the typical user is served by the nearest BS at x_0 , (6) becomes

$$\begin{aligned}\bar{F}_{\hat{R}_s}(R_0) &= \mathbb{P}(\|e^*(x_0) - x_0\| > \beta^{1/\alpha}\|x_0\|) \\ &\stackrel{(a)}{=} \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}r_u); r_u < \beta^{-\frac{1}{\alpha}}D_{\min}] \\ &= \int_0^\infty \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}r_u); D_{\min} > \beta^{\frac{1}{\alpha}}r_u \mid r_u = y] f_{r_u}(y) dy, \quad (33)\end{aligned}$$

where step (a) is based on the fact that eavesdroppers are assumed to be lied in the cell boundaries for the worst case. The probability expression herein can be further derived as

$$\begin{aligned}&\mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}r_u); D_{\min} > \beta^{\frac{1}{\alpha}}r_u \mid r_u = y] \\ &\stackrel{(b)}{=} \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}y)] \cdot \mathbb{P}(D_{\min} > \beta^{\frac{1}{\alpha}}y \mid r_u = y) \\ &\geq \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}y)] \cdot \mathbb{P}(D_{\min} > \beta^{\frac{1}{\alpha}}y) \\ &= \exp(-\pi\lambda_e(\beta^{\frac{1}{\alpha}}y)^2) \int_{\beta^{\frac{1}{\alpha}}y}^\infty f_{D_{\min}}(z) dz \\ &= \exp(-\pi(\lambda_e + 4\lambda_{BS})\beta^{\frac{2}{\alpha}}y^2), \quad (34)\end{aligned}$$

where the independence between Φ_e and Φ_{BS} is used to separate the two probability expressions in step (b), and the former part is only dependent on the density of eavesdroppers λ_e and the ball's area $\pi\beta^{2/\alpha}y^2$, but independent of x_0 . It should be noticed that the value of r_u has an impact on the distribution of D_{min} , and we need to use $f_{D_{min}|r_u}(\cdot|\cdot)$ to derive $\mathbb{P}(D_{min} > \beta^{\frac{1}{\alpha}}y \mid r_u = y)$ in step (b). Because the tractable result of $f_{D_{min}|r_u}(\cdot|\cdot)$ is not available, we obtain a lower bound (also served as a tractable approximation) expression by ignoring the impact of r_u on the distribution of D_{min} , due to the fact that $\mathbb{P}(D_{min} > x \mid r_u = y) \geq \mathbb{P}(D_{min} > x)$. The lower bound by replacing distribution $f_{D_{min}}(\cdot)$ can provide a good approximation, which will be demonstrated by the numerical comparisons in Section IV.

By substituting (34) and the pdf of r_u given in (9) into (33), the lower bound expression (32) can be obtained, which completes the proof. ■

Remark: When $\lambda_e \gg \lambda_{BS}$, the impact of cell boundaries on the secrecy rate becomes negligible, since almost surely an eavesdropper exists inside the ball $\mathcal{B}(x_0, D_{min})$ and limits the achievable secrecy rate, then making (32) become (8).

Corollary 3. *Under the conditions of mobile users being served by the nearest BS and only intracell eavesdroppers' location information available, a lower bound of the average secrecy rate achievable at the typical user is provided by*

$$\mathbb{E}[\hat{R}_s] \geq \frac{\alpha}{2 \ln 2} \cdot \ln \left(\frac{5\lambda_{BS} + \lambda_e}{4\lambda_{BS} + \lambda_e} \right). \quad (35)$$

Proof: The lower bound of the average secrecy rate $\mathbb{E}[\hat{R}_s]$ can be derived by integrating (32) from 0 to ∞ . Since the integrand in this integral has the similar form as (8), the same deduction procedure can be performed to obtain this lower bound. ■

Remark: Under the condition of mobile users camping on the nearest BS, Scenario-I and this case can be regarded as two extremes: in the former scenario, the location information of all eavesdroppers is shared among BSs, while no location and identity information exchange is allowed in the latter one. By comparing the expressions of (11) with (35), it is easy to conclude that the latter case's average secrecy rate achievable increases with λ_{BS}/λ_e much slower than the counterpart in Scenario-I. This trend, which will be given numerically in following Section IV, demonstrates the impact of the location and identity information exchange between BSs.

2) *Location and identity information exchange limited with neighboring cells only:* In order to further characterize how the availability of the location and identity information affects the secrecy performance, we will investigate the secrecy rate for the case where the location information and identity exchange is restricted to the serving BS's neighboring cells only.

Given certain neighboring BSs participating in the information exchange with the serving BS, the region outside the cells covered by these BSs is the unknown region. By considering the worst case scenario that the eavesdroppers can be located anywhere inside the unknown region, the secrecy performance is limited by the minimum distance from the unknown region to the serving BS. As long as the minimum distance is the same, the secrecy performance stays the same regardless of the shape of the unknown region, which means that the consideration of a disk-shape known region does not lose the generality of the result on secrecy rates. Therefore, we apply the following model to represent the known and unknown regions: only the location information of the eavesdroppers with distances less than D_0 from the serving BS is available to it, i.e., the eavesdroppers outside the region $\mathcal{B}(x, D_0)$ are unknown to a BS at x . The value D_0 is called *detection radius* in our analysis.

From a network design perspective, a larger D_0 represents information exchanging feasible with BSs farther away, and in other words, a larger D_0 means that more BSs participate in the information exchange with the serving BS. This scenario provides limited information exchange, which can be regarded as an intermediate case between Scenario-II and Scenario-III(1), and reflects practical considerations, such as the limited bandwidth of the backhaul network and the complexity introduced by extensive information sharing in the practical implementation. By investigating how the achievable secrecy rate changes with D_0 , one can obtain insights on the improvement of the secrecy performance as more BSs participate in the information exchange process.

Proposition 5. *Under the conditions of mobile users being served by the nearest BS and the detection radius is D_0 , the CCDF of the achievable secrecy rate obtained at the typical user is given by*

$$\bar{F}_{\hat{R}_s}(R_0) = \left(1 - \exp \left[-\pi(\lambda_e + \lambda_{BS} 2^{-\frac{2R_0}{\alpha}}) D_0^2 \right] \right) \cdot \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2R_0)/\alpha}}, \quad \text{for } R_0 \geq 0. \quad (36)$$

Proof: Based on the available location information of eavesdroppers with distances less

than D_0 and the typical user served by the nearest BS at x_0 , (6) can be derived as

$$\begin{aligned}
\bar{F}_{\hat{R}_s}(R_0) &= \mathbb{P}\left(\|e^*(x_0) - x_0\| > \beta^{1/\alpha}\|x_0\|\right) \\
&= \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}r_u); r_u < \beta^{-\frac{1}{\alpha}}D_0] \\
&= \int_0^{\beta^{-\frac{1}{\alpha}}D_0} \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}r_u) \mid r_u = y] f_{r_u}(y) dy \\
&\stackrel{(a)}{=} \int_0^{\beta^{-\frac{1}{\alpha}}D_0} \mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}y)] f_{r_u}(y) dy \\
&\stackrel{(b)}{=} \int_0^{2^{-\frac{R_0}{\alpha}}D_0} 2\pi\lambda_{BS}y \cdot \exp(-\pi\lambda_e 2^{\frac{2R_0}{\alpha}}y^2 - \pi\lambda_{BS}y^2) dy \\
&= \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2R_0)/\alpha}} \cdot \left(1 - \exp\left[-\pi(\lambda_e + \lambda_{BS} 2^{-\frac{2R_0}{\alpha}})D_0^2\right]\right), \quad (37)
\end{aligned}$$

where step (a) follows the independence between Φ_e and Φ_{BS} , and step (b) is derived based on the void probability of PPP and the pdf of r_u . It should be noticed that the probability expression $\mathbb{P}[\text{No Eve in } \mathcal{B}(x_0, \beta^{\frac{1}{\alpha}}y)]$ is only dependent on the density of eavesdroppers λ_e and the ball's area $\pi\beta^{2/\alpha}y^2$, but independent of x_0 . The integration from 0 to $2^{-\frac{R_0}{\alpha}}D_0$ gives the result which completes the proof. \blacksquare

Remark: As expected, the general trend can be understood as follows: when detection radius D_0 decreases, the location information of eavesdroppers surrounding the serving BS reduces, which makes a lower probability to maintain the secrecy rate R_0 . As we increase D_0 to infinity, the condition turns to be the same as Scenario-I, thus making (36) become (8).

Corollary 4. *Under the conditions of mobile users being served by the nearest BS and the detection radius is D_0 , the average secrecy rate achievable at the typical user is provided by*

$$\mathbb{E}[\hat{R}_s] = \frac{\alpha}{2\ln 2} \cdot \ln\left(\frac{\lambda_{BS} + \lambda_e}{\lambda_e}\right) - \frac{\alpha}{2\ln 2} \cdot \left[E_1(\pi\lambda_e D_0^2) - E_1(\pi(\lambda_e + \lambda_{BS})D_0^2)\right]. \quad (38)$$

Proof: Based on the CCDF expression given in Proposition 5, the average secrecy rate achievable at the typical user can be provided by integrating (36) from 0 to ∞ , i.e.,

$$\begin{aligned}
\mathbb{E}[\hat{R}_s] &= \int_0^\infty \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2t)/\alpha}} \cdot \left(1 - \exp\left[-\pi(\lambda_e + \lambda_{BS} 2^{-\frac{2t}{\alpha}})D_0^2\right]\right) dt \\
&= \int_0^\infty \frac{1}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2t)/\alpha}} dt - \int_0^\infty \frac{\exp\left[-\pi(\lambda_e + \lambda_{BS} 2^{-\frac{2t}{\alpha}})D_0^2\right]}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2t)/\alpha}} dt \\
&\stackrel{(a)}{=} \frac{\alpha}{2\ln 2} \cdot \ln\left(\frac{\lambda_{BS} + \lambda_e}{\lambda_e}\right) - \\
&\quad \exp(-\pi\lambda_e D_0^2) \int_0^\infty \frac{\exp\left[-\pi\lambda_{BS} D_0^2 \cdot 2^{-\frac{2t}{\alpha}}\right]}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2t)/\alpha}} dt, \quad (39)
\end{aligned}$$

where the deduction of the former part in step (a) utilizes the result solved in Corollary 1, and then we will focus on the integral in its latter part, i.e.,

$$\begin{aligned}
& \exp(-\pi\lambda_e D_0^2) \int_0^\infty \frac{\exp[-\pi\lambda_{BS} D_0^2 \cdot 2^{-\frac{2t}{\alpha}}]}{1 + \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2t)/\alpha}} dt \\
\stackrel{(b)}{=} & \exp(-\pi\lambda_e D_0^2) \int_{\frac{\lambda_e}{\lambda_{BS}}}^\infty \frac{\exp(-\pi\lambda_e D_0^2 v^{-1})}{1+v} \cdot \frac{\alpha}{2v \ln 2} dv \\
\stackrel{(c)}{=} & \frac{\alpha}{2 \ln 2} \int_{\pi\lambda_e D_0^2}^{\pi(\lambda_{BS}+\lambda_e)D_0^2} \frac{1}{s \exp(s)} ds \\
= & \frac{\alpha}{2 \ln 2} \left[E_1(\pi\lambda_e D_0^2) - E_1(\pi(\lambda_e + \lambda_{BS})D_0^2) \right], \tag{40}
\end{aligned}$$

where step (b) and step (c) are obtained by employing changes of variables $v = \frac{\lambda_e}{\lambda_{BS}} \cdot 2^{(2t)/\alpha}$ and $s = \frac{\pi\lambda_e D_0^2}{v} + \pi\lambda_e D_0^2$ respectively, and the last step can be derived by using the definition of the exponential integral. Plugging (40) into (39) gives the desired result in (38), which completes the proof. ■

IV. NUMERICAL ILLUSTRATIONS

In this section, we present numerical results on the achievable secrecy rate for all three major scenarios respectively. Here we define the value SNR as the received SNR from the serving BS at the distance $r = 1$, i.e., $\text{SNR} = P_{BS}/\sigma^2$. All simulation results are conducted under a high SNR condition, i.e., $\text{SNR} = 20\text{dB}$, and unitary BS density, i.e., $\lambda_{BS} = 1$, to compare with our analysis for the purpose of model validation.

Firstly, for each curve in Fig. 4, we show the average secrecy rates achievable at the typical user in Scenario-I, for both path loss exponents of $\alpha = 4$ and $\alpha = 2.5$. As can be seen in this figure, the curves representing the analytical expression (11) in Corollary 1 match the simulated results for all conditions.

Fig. 5 and Fig. 6 demonstrate the results of Scenario-II, the optimal case where all mobile users' location and identity information is completely known and the optimal BS is chosen to maximize the achievable secrecy rate. Fig. 5 shows the typical user's secure link coverage probability with the threshold $R_0 = 0$ or $R_0 = 5$ to claim outage. Note that the upper bound in Proposition 3 converges to the exact coverage probability in the special case of $R_0 = 0$, which can be observed from the fact that the curves representing the approximation (23) based on Proposition 3 match the simulated results in Fig. 5. However, this approximation is not precise for large values of R_0 , e.g., $R_0 = 5$ and the analytical reason for this inaccuracy is explained in remark after Proposition 3. On the other hand, the lower bound and the upper bound

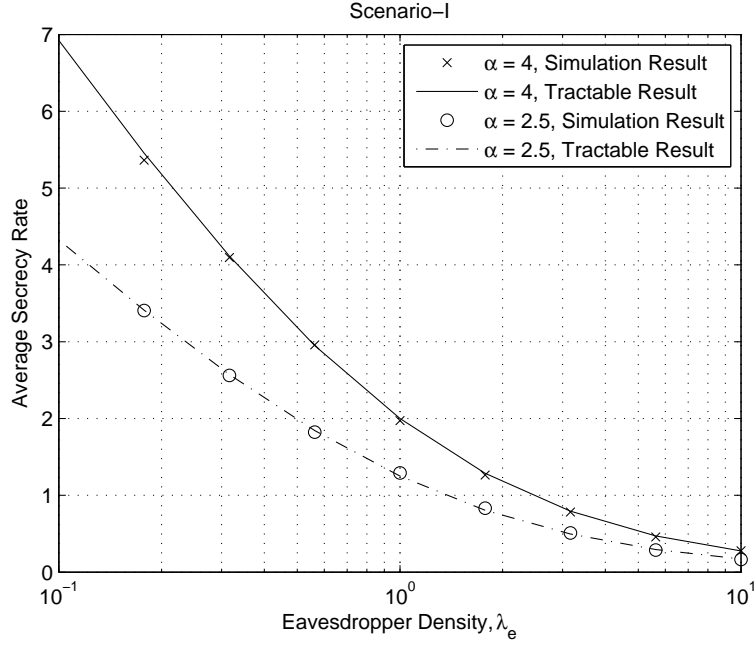


Fig. 4. The average secrecy rate achievable versus the eavesdropper density λ_e for Scenario-I (full location information; nearest BS to serve). Simulation and tractable analytical results are shown for different path loss exponents α .

in Proposition 2 tend to give more accurate approximations of the exact secrecy coverage probability for large values of R_0 , which can be regarded as a complementary property to offset the limitation of the upper bound in Proposition 3 mentioned above. From the results shown in Fig. 6, the tractable upper and lower bounds of the achievable secrecy rates in Corollary 2 are also reasonably accurate. Furthermore, the approximations for the average secrecy rates achievable based on Proposition 3 are also demonstrated in Fig. 6 and turn out to be inaccurate due to Proposition 3's imprecise estimate for large R_0 . The achievable secrecy rate given in Scenario-II provides the maximum value over all the scenarios considered in this paper.

By comparing Fig. 4 with Fig. 6, it can be noted that picking the nearest BS to serve can achieve a secrecy rate nearly as much as the optimal value. For example, the secrecy rate in Scenario-I is approximately 1.9 for $\alpha = 4$ and the eavesdroppers' density $\lambda_e = 1$, compared with around 2.1 for the optimal case in Scenario-II. In other words, there is only marginal benefits from optimally choosing the serving BS instead of simply picking the nearest BS to serve.

Fig. 7 shows the average secrecy rate achievable for Scenario-III(1), where no location and identity information exchange is allowed and only intracell users' location information

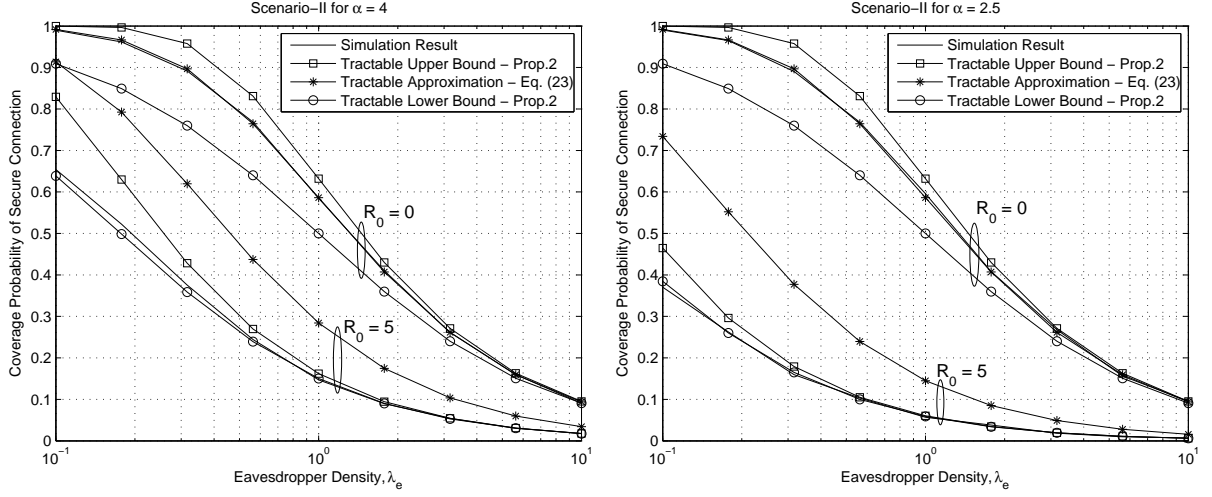


Fig. 5. The secure coverage probability versus the eavesdropper density λ_e for Scenario-II (full location information; optimal BS to serve). Simulation and tractable analytical results are shown for different thresholds $R_0 = 0$ or 5 to claim outage. Different path loss exponents are demonstrated: $\alpha = 4$ (left) and $\alpha = 2.5$ (right).

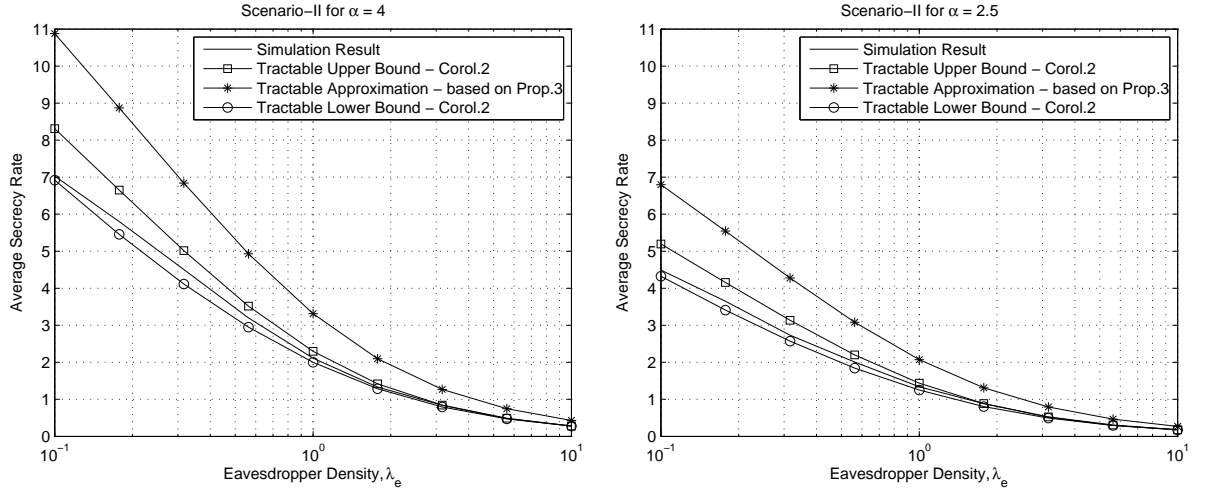


Fig. 6. The average secrecy rate achievable versus the eavesdropper density λ_e for Scenario-II (full location information; optimal BS to serve). Simulation and tractable analytical results are shown for different path loss exponents: $\alpha = 4$ (left) and $\alpha = 2.5$ (right).

is known to the serving BS. Due to the shrinkage of the region where location information is available, the secrecy performance is significantly degraded compared with the counterpart in Fig. 4. For example, the average secrecy rate achievable is around 0.57 for $\alpha = 4$ and $\lambda_e = 1$, whereas the corresponding value can reach around 1.9 for Scenario-I. We also observe a relatively slow drop in the average secrecy rate achievable as λ_e changes from 0.1 toward 1, due to its weak dependence on the density of eavesdroppers in this range of λ_e , which

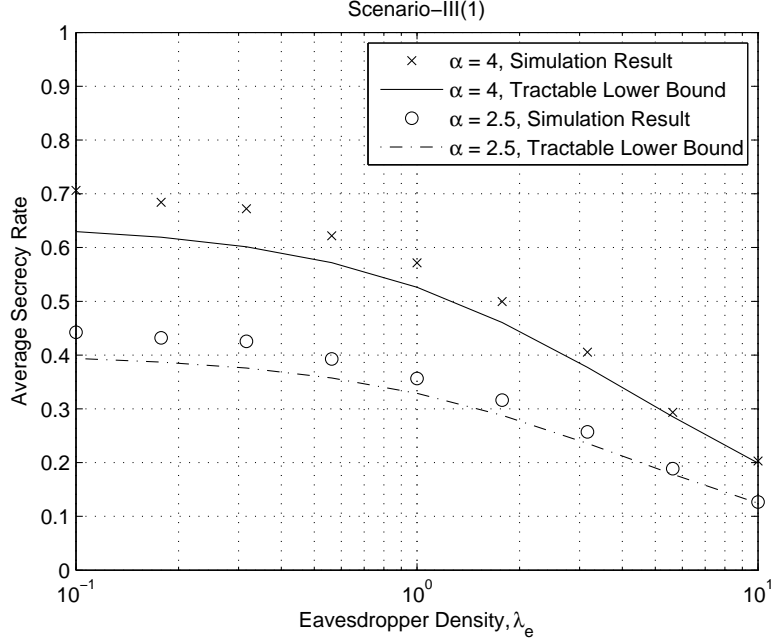


Fig. 7. The average secrecy rate achievable versus the eavesdropper density λ_e for Scenario-III(1) (no location information exchange; nearest BS to serve). Simulation results and tractable lower bounds are shown for different path loss exponents α .

suggests that the lack of location information outside the serving BS's cell becomes the main restrictive factor in determining the secrecy performance. On the other hand, as λ_e increases from 1 to 10, the average secrecy rate achievable accelerates to drop since the eavesdropper density is more influential. It can be shown that the tractable lower bound in (35) captures the general trend of the curves and can be used as a tool to make a precise estimate.

Furthermore, by presenting the average secrecy rate achievable versus the detection radius D_0 in Fig. 8, we can see the importance of eavesdroppers' location information on the secrecy performance. In case of relatively small values of D_0 , any increase of the detection radius brings remarkable benefit to the achievable secrecy rate. On the other hand, in case of large D_0 , any further increase in the detection radius does not substantially impact the secrecy rate, since the eavesdropper that limits the secrecy performance is usually located not too far away from the serving BS and its distance is likely to be smaller than D_0 when D_0 is sufficiently large. Take the curve with $\alpha = 4$ and $\lambda_e = 0.1$ for instance, the secrecy performance improves significantly as D_0 is increased up to 2, and any further increase from $D_0 = 2$ has a limited effect. This performance trend over the range of detection radius can be utilized to appropriately choose the number of neighboring BSs for the information

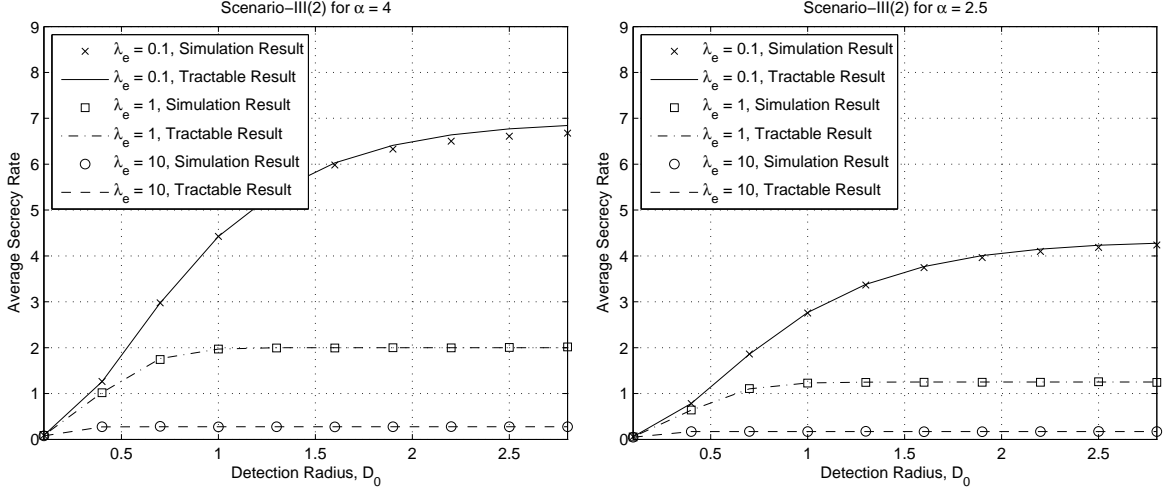


Fig. 8. The average secrecy rate achievable versus the detection radius D_0 for Scenario-III(2) (location information for users with distances less than D_0 ; nearest BS to serve). Simulation and tractable analytical results are shown for different eavesdropper densities λ_e and different path loss exponents: $\alpha = 4$ (left) and $\alpha = 2.5$ (right).

exchange in order to achieve a good secrecy performance whilst taking the implementation cost of such information exchange into consideration. It should be noticed that the slight mismatches between simulation and tractable results in Fig. 4 and Fig. 8 come from the high SNR assumption used in our analysis, and become almost invisible at $\text{SNR} = 30\text{dB}$ (plots omitted for brevity).

Another fact clearly shown from Fig. 6-8 is that better performance can be obtained for larger values of path loss exponent α , e.g., the average secrecy rate achievable is higher for $\alpha = 4$ than the counterpart for $\alpha = 2.5$. This is because the resultant larger path loss from larger α indicates worse signal condition to both the eavesdroppers and the typical user, whereas the former effect turns out to be more influential on the secrecy performance.

V. CONCLUSION

In this work, we studied the secrecy performance of cellular networks considering cell association and information exchange between BSs potentially provided by the carrier-operated high-speed backhaul and core-networks. Using the stochastic geometry modeling of cellular networks, tractable results to characterize the secrecy rate were obtained under different assumptions on the cell association and location information exchange between BSs. The simulation results validate the tractable expressions and approximations. From the analysis in this paper, we identified the unique feature for secure transmissions that the optimal BS

is often not the nearest BS. Nevertheless, our result shows that keeping the nearest BS to be used for secure transmissions still achieves near-optimal secrecy performance. We also considered the exchange of eavesdropper's location information between BSs and studied its impact on the secrecy rate performance. Our finding is that it is usually sufficient to allow a small number of neighboring BSs to exchange the location information for achieving close to maximum secrecy rate. Specifically, our analytical result provides network designers practical guidelines to decide the necessary information exchange range, i.e., how many nearby BSs should participate in the information exchange for achieving a certain level of secrecy performance.

The result in this work applies to scenarios where a carefully planned frequency reuse pattern is assumed, and the serving BS can occupy some resource blocks exclusively in a relatively large region. In future cellular networks, however, interference will become an important factor. Since the channel conditions of both legitimate users and eavesdroppers will be degraded by introducing interference, the impact of the co-channel interference on the secrecy performance of large-scale cellular network is still unknown. Another limitation is that the BS cooperation considered in this paper is confined to cell association and location information exchange. Coordinated multipoint (CoMP) transmission, as an emerging BS cooperation technique in future cellular networks, can be potentially utilized, and its benefit on the secrecy performance is an interesting problem to investigate.

REFERENCES

- [1] 3GPP Tech. Spec. 33.102 V8.6.0, "3G security; Security architecture."
- [2] C. B. Sankaran, "Network access security in next-generation 3GPP systems: A tutorial," *IEEE Commun. Mag.*, vol. 47, no. 2, pp. 84–91, Feb. 2009.
- [3] A. D. Wyner, "The wire-tap channel," *Bell System Technical Journal*, vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
- [4] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," *IEEE Trans. Inform. Theory*, vol. 24, no. 3, pp. 339–348, May 1978.
- [5] M. Haenggi, "The secrecy graph and some of its properties," in *Proc. IEEE Int'l Symp. on Information Theory (ISIT'08)*, Toronto, Canada, July 2008, pp. 539–543.
- [6] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks - Part I: Connectivity," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 125–138, Feb. 2012.
- [7] S. Goel, V. Aggarwal, A. Yener, and A. R. Calderbank, "Modeling location uncertainty for eavesdroppers: A secrecy graph approach," in *Proc. IEEE Int'l Symp. on Information Theory (ISIT'10)*, Austin, USA, June 2010, pp. 2627–2631.
- [8] P. C. Pinto and M. Z. Win, "Continuum percolation in the intrinsically secure communications graph," in *Proc. 2010 Int'l Symp. on Information Theory and its Applications (ISITA'10)*, Taichung, Taiwan, Oct. 2010, pp. 349–354.
- [9] X. Zhou, R. K. Ganti, and J. G. Andrews, "Secure wireless network connectivity with multi-antenna transmission," *IEEE Trans. Wireless Commun.*, vol. 10, no. 2, pp. 425–430, Feb. 2011.

- [10] P. C. Pinto, J. Barros, and M. Z. Win, "Secure communication in stochastic wireless networks - Part II: Maximum rate and collusion," *IEEE Trans. Inform. Forensics and Security*, vol. 7, no. 1, pp. 139–147, Feb. 2012.
- [11] O. O. Koyluoglu, C. E. Koksal, and H. E. Gamal, "On secrecy capacity scaling in wireless networks," *IEEE Trans. Inform. Theory*, vol. 58, no. 5, pp. 3000–3015, May 2012.
- [12] Y. Liang, H. Poor, and L. Ying, "Secrecy throughput of MANETs with malicious nodes," in *Proc. IEEE Int'l Symp. on Information Theory (ISIT'09)*, Seoul, Korea, June 2009, pp. 1189–1193.
- [13] C. Capar, D. Goeckel, B. Liu, and D. Towsley, "Secret communication in large wireless networks without eavesdropper location information," in *Proc. 31st Annual IEEE Int'l Conf. on Computer Commun. (IEEE INFOCOM'12)*, Orlando, USA, Mar. 2012, pp. 1152–1160.
- [14] X. Zhou, R. K. Ganti, J. G. Andrews, and A. Hjørungnes, "On the throughput cost of physical layer security in decentralized wireless networks," *IEEE Trans. Wireless Commun.*, vol. 10, no. 8, pp. 2764–2775, Aug. 2011.
- [15] —, "Secrecy transmission capacity of decentralized wireless networks," in *Proc. 49th Annual Allerton Conference on Communication, Control, and Computing (Allerton'11)*, Monticello, USA, Sept. 2011, pp. 1726–1732.
- [16] D. Stoyan, W. S. Kendall, and J. Mecke, *Stochastic Geometry and its Applications*, 2nd ed. New York, NY: John Wiley & Sons Ltd., 1995.
- [17] F. Baccelli and B. Błaszczyszyn, *Stochastic Geometry and Wireless Networks, Volume I: Theory*, 1st ed. Hanover, MA: Now Publishers Inc., 2009.
- [18] T. X. Brown, "Cellular performance bounds via shotgun cellular systems," *IEEE J. Select. Areas Commun.*, vol. 18, no. 11, pp. 2443–2455, Nov. 2000.
- [19] X. Yang and A. P. Petropulu, "Co-channel interference modeling and analysis in a Poisson field of interferers in wireless communications," *IEEE Trans. Signal Processing*, vol. 51, no. 1, pp. 64–76, Jan. 2003.
- [20] M. Haenggi, "A geometric interpretation of fading in wireless networks: Theory and applications," *IEEE Trans. Inform. Theory*, vol. 54, no. 12, pp. 5500–5510, Dec. 2008.
- [21] J. G. Andrews, F. Baccelli, and R. K. Ganti, "A tractable approach to coverage and rate in cellular networks," *IEEE Trans. Commun.*, vol. 59, no. 11, pp. 3122–3134, Nov. 2011.
- [22] H. S. Dhillon, R. K. Ganti, F. Baccelli, and J. G. Andrews, "Modeling and analysis of K-tier downlink heterogeneous cellular networks," *IEEE J. Select. Areas Commun.*, vol. 30, no. 3, pp. 550–560, Apr. 2012.
- [23] W. C. Cheung, T. Q. Quek, and M. Kountouris, "Throughput optimization, spectrum allocation, and access control in two-tier femtocell networks," *IEEE J. Select. Areas Commun.*, vol. 30, no. 3, pp. 561–574, Apr. 2012.
- [24] C. S. Chen, V. M. Nguyen, and L. Thomas, "On small cell network deployment: A comparative study of random and grid topologies," in *Proc. IEEE 76th Vehic. Tech. Conf. (VTC'12-Fall)*, Québec City, Canada, Sept. 2012, pp. 1–5.
- [25] S. M. Yu and S.-L. Kim, Downlink capacity and base station density in cellular networks. [Online]. Available: <http://arxiv.org/abs/1109.2992>
- [26] A. Sarkar and M. Haenggi, "Secrecy Coverage," *Internet Mathematics*, 2012, accepted. Available at <http://www.nd.edu/~mhaenggi/pubs/im12.pdf>.
- [27] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," *IEEE Trans. Inform. Theory*, vol. 54, no. 6, pp. 2515–2534, June 2008.
- [28] M. Haenggi, "On distances in uniformly random networks," *IEEE Trans. Inform. Theory*, vol. 51, no. 10, pp. 3584–3586, Oct. 2005.
- [29] A. Jeffrey and H.-H. Dai, *Handbook of mathematical formulas and integrals*, 4th ed. Burlington, MA: Academic Press, 2008.
- [30] A. Okabe, B. Boots, and K. Sugihara, *Spatial Tessellations: Concepts and Applications of Voronoi Diagrams*, 1st ed. West Sussex, England: John Wiley & Sons Ltd., 1992.

- [31] A. L. Hinde and R. E. Miles, “Monte Carlo estimates of the distributions of the random polygons of the Voronoi tessellation with respect to a Poisson process,” *Journal of Statistical Computation and Simulation*, vol. 10, no. 3-4, pp. 205–223, 1980.
- [32] D. Weaire, J. P. Kermode, and J. Wejchert, “On the distribution of cell areas in a Voronoi network,” *Philosophical Magazine Part B*, vol. 53, no. 5, pp. L101–L105, 1986.
- [33] M. Abramowitz and I. Stegun, *Handbook of mathematical functions: with formulas, graphs, and mathematical tables*, 1st ed. Mineola, NY: Dover Publications, 1965.